Math 116: Problem Set 1

Owen Jones

1/14/2024

1. (a) $543 \equiv 3 \pmod{12}, 379 \equiv 7 \pmod{12} \Rightarrow 543 \cdot 379 \equiv 21 \pmod{12}$
   $\Rightarrow 543 \cdot 379 \equiv 9 \pmod{12}$

   (b) $29513 \equiv 13 \pmod{100}, 93723208 \equiv 8 \pmod{100}$
   $\Rightarrow 29513 \cdot 93723208 \equiv 104 \pmod{100}$
   $\Rightarrow 29513 \cdot 93723208 \equiv 4 \pmod{100}$

   (c) $24637 \equiv 7 \pmod{15} \Rightarrow 24637^3 \equiv 343 \pmod{15}$
   $\Rightarrow 24637^3 \equiv 13 \pmod{15}$

   (d) $82375 = 4576 \cdot 18 + 7 \Rightarrow 82375 \equiv 7 \pmod{18}$
   $\Rightarrow 82375^3 \equiv 343 \pmod{18}$
   $343 = 19 \cdot 18 + 1 \Rightarrow 82375^3 \equiv 1 \pmod{18}$
   $5628 = 1876 \cdot 3 \Rightarrow 82375^{5628} \equiv 1^{1876} \pmod{18}$
   $\Rightarrow 82375^{5628} \equiv 1 \pmod{18}$

   (e) $46249 = 2569 \cdot 18 + 7 \Rightarrow 46249 \equiv 7 \pmod{18}$
   $\Rightarrow 46249^3 \equiv 1 \pmod{18}$
   $601 = 200 \cdot 3 + 1 \Rightarrow 46249 \cdot 46249^{3 \cdot 200} \equiv 7 \cdot 1^{200} \pmod{18}$
   $\Rightarrow 46249^{601} \equiv 7 \pmod{18}$

2. (a) $\gcd(128, 69) = \gcd(69, 59) = \gcd(59, 10) = \gcd(10, 9) = \gcd(9, 1) = 1$
   $1 = 10 - 9 = 69 - 2 \cdot 59 + 5 \cdot 10 = 8 \cdot 69 - 2 \cdot 128 - 5 \cdot 59 = 13 \cdot 69 - 7 \cdot 128$
   Let $d = 13$

   (b) $84 \cdot 69 \cdot 13 \equiv 84 \pmod{128} \Rightarrow 68 \cdot 69 \equiv 84 \pmod{128}$
   $107 \cdot 69 \cdot 13 \equiv 107 \pmod{128} \Rightarrow 111 \cdot 69 \equiv 107 \pmod{128}$
   $38 \cdot 69 \cdot 13 \equiv 38 \pmod{128} \Rightarrow 110 \cdot 69 \equiv 38 \pmod{128}$
   $3 \cdot 69 \cdot 13 \equiv 3 \pmod{128} \Rightarrow 39 \cdot 69 \equiv 3 \pmod{128}$
   $68 \cdot 69 \cdot 13 \equiv 68 \pmod{128} \Rightarrow 116 \cdot 69 \equiv 68 \pmod{128}$
   $32 \cdot 69 \cdot 13 \equiv 32 \pmod{128} \Rightarrow 32 \cdot 69 \equiv 32 \pmod{128}$
   $58 \cdot 69 \cdot 13 \equiv 58 \pmod{128} \Rightarrow 114 \cdot 69 \equiv 58 \pmod{128}$
   $127 \cdot 69 \cdot 13 \equiv 127 \pmod{128} \Rightarrow 115 \cdot 69 \equiv 9 \pmod{128}$
   $25 \cdot 69 \cdot 13 \equiv 25 \pmod{128} \Rightarrow 69 \cdot 69 \equiv 25 \pmod{128}$
   $78 \cdot 69 \cdot 13 \equiv 78 \pmod{128} \Rightarrow 118 \cdot 69 \equiv 118 \pmod{128}$
   $57 \cdot 69 \cdot 13 \equiv 57 \pmod{128} \Rightarrow 101 \cdot 69 \equiv 57 \pmod{128}$
   The message is: Don't trust Eve

3. (a) **reflexive:** $(a - a) = 0$, $0 \in \mathbb{Z}$, and $n \cdot 0 = 0$ for any integer n.

(b) **symmetric:** Given $a \equiv b \pmod{n}$. If $n \mid (a-b)$ then $\exists k \in \mathbb{Z}$ s.t $(a-b) = kn$. If $\exists k \in \mathbb{Z}$ then $\exists -k \in \mathbb{Z}$ s.t $(b-a) = -kn \Rightarrow n \mid (b-a) \Leftrightarrow b \equiv a \pmod{n}$.

(c) **transitive** If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $\exists k_1, k_2 \in \mathbb{Z}$ s.t $a-b = k_1 n$ and $b-c = k_2 n$. Because $\exists k_1+k_2 \in \mathbb{Z}$ s.t $a-c = (k_1+k_2)n$, we can say $a \equiv c \pmod{n}$

4. If $n \mid (a-a')$ and $n \mid (b-b')$ then there exists $k_1, k_2 \in \mathbb{Z}$ s.t $a - a' = k_1 n$ and $b-b' = k_2 n$. It follows $(a-b)-(a'-b') = (k_1-k_2)n$ where $k_1-k_2 \in \mathbb{Z}$. Thus, $n \mid (a-b)-(a'-b') \Rightarrow a-b \equiv a'-b' \pmod{n}$

5. (a) Let $X = \mathbb{R}^+ \cup \{0\}$ and $Y = \mathbb{R}$. Let $e : X \to Y = \sqrt{x}$ and $d : Y \to X = y^2$. $d(e(x)) = (\sqrt{x})^2 = x \; \forall x \in X$, but $e(d(-1)) = \sqrt{(-1)^2} = 1$, so $e(d(y)) \neq 1_Y$

   (b) WLOG let $|X| = |Y| = n$. Suppose f is one-to-one. Moreover, each element of X needs to map to a different element of Y. Because there are n elements in the set X, n elements of the set Y will have elements of X that map to them. However, Y only contains n elements, so for every element $y \in Y$, $\exists x \in X$ s.t $f(x) = y$.

   (c) Let $E_k : \mathcal{P} \to \mathcal{C}$ and $D_k : \mathcal{C} \to \mathcal{P}$ where $D_k(E_k(m)) = m$ for each $m \in \mathcal{C}$. It follows $E_k(D_k(E_k(m))) = E_k(m)$ where $m \in \mathcal{C}$. E_k must be injective because if $E_k(m) = n$ and $E_k(m') = n$, then either $D_k(E_k(m)) \neq m$ or $D_k(E_k(m')) \neq m'$ because $D_K(n)$ cannot map to two different values. Because $\mathcal{P}$ and $\mathcal{C}$ are of the same size, part (b) says that E_k is onto, so for every $n \in \mathcal{P}$, there exists $m \in \mathcal{C}$ s.t $n = E_k(m)$. Thus, $E_k(D_k(n)) = n$.